



TITLE:

Integers in p -adically closed fields are definable (Model Theory of fields and its applications)

AUTHOR(S):

Itai, Masanori; Ochi, Yoshihiro

CITATION:

Itai, Masanori ...[et al.]. Integers in p -adically closed fields are definable (Model Theory of fields and its applications). 数理解析研究所講究録 2006, 1515: 50-51

ISSUE DATE:

2006-09

URL:

<http://hdl.handle.net/2433/58698>

RIGHT:

Integers in p -adically closed fields are definable

Masanori Itai* (板井 昌典 東海大学 理学部)

Yoshihiro Ochi† (越智 禎宏 東京電機大学 理工学部)

Abstract

We show that the integers in p -adically closed fields are definable.

1 Theory of p -adically closed fields

In this short memo we show that the integers in p -adically closed fields are definable. This is a simple generalization of the fact that the integers in \mathbb{Q}_p are definable.

First we need to fix a language for the model theory of p -adically closed fields.

The language $\mathcal{L}_R = \{+, -, \cdot, ^{-1}, R, P_n (n \in \mathbb{N}), 0, 1, \pi, u_1, \dots, u_{d-1}\}$, where R and P_n are unary predicates, π, u_1, \dots, u_{d-1} are constants.

The axiom of p -adically closed fields is the infinite set of following sentences.

- theory of fields of characteristic zero
- $\forall x (x \neq 0 \rightarrow R(x) \vee R(x^{-1}))$
- $\forall x (P_n(x) \leftrightarrow \exists y (y^n = x))$ for each n .
- π is a *prime* element: this means that $v(\pi)$ is the least positive element, i.e., $v(\pi) > 0 \wedge \forall x (v(x) \geq 0 \rightarrow v(\pi) < v(x))$ which can be expressed by $R(\pi) \wedge \neg R(\pi^{-1}) \wedge \forall x (R(x) \rightarrow R(x\pi^{-1}) \wedge \neg R(\pi x^{-1}))$ (for the definition of a prime element, see p. 13 of [1])
- p -valued field: this can be expressed by saying that the value group is a \mathbb{Z} -group, i.e., for each natural number n the following holds, $\forall a \exists x (R(a(\pi^i x^n)^{-1}) \wedge R(\pi^i x^n a^{-1}))$ with some $i \in \{0, 1, \dots, n-1\}$. (see, p. 85 of [1])
- p -rank d : with $d-1$ constants express that \mathcal{O}/p is a d -dimensional vector space over \mathbb{Z}/p , i.e., $\forall x (R(x) \rightarrow x/p = a_0 + a_1 u_1 + \dots + a_d u_d)$ with $a_i \in \{0, 1, \dots, p-1\}$.
- Hensel's lemma holds; this can be expressed by saying that Newton's lemma holds, i.e., for each $f(X) \in \mathcal{O}[X]$, if there exists $a \in \mathcal{O}$ such that $v(f(a)) > v(f'(a)^2)$ then there is an x such that $f(x) = 0$. Therefore for each natural number n we write down the following: $\forall a_1 \dots \forall x_n \exists a (R(a_1) \wedge \dots \wedge R(a_n) \wedge R(a) \rightarrow R((a^n + a_1 a^{n-1} + \dots + a_{n-1} a + a_n)(na^{n-1} + (n-1)a^{n-2} a_1 + \dots + a_{n-1})^{-2}) \wedge \neg R((na^{n-1} + (n-1)a_1 a^{n-2} + \dots + a_{n-1})(a^n + a_1 a^{n-1} + \dots + a_{n-1} a + a_n)^{-1})) \rightarrow \exists x (x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n = 0)$

Remark 1 Recall that the p -adic Kochen operator can characterize formally p -adic fields of type (e, f) , see Lemma 6.1 of p. 93 [1].

*Tokai University

†Tokyo Denki University

2 Defining the ring of integers in the p -adically closed fields

It is well known that the ring of integers \mathbb{Z}_p is definable in terms of the ring language in the p -adic numbers \mathbb{Q}_p . We show in this section that if K is a p -adically closed field the ring of integers \mathcal{O}_K is also definable in the ring language.

Let K be a p -adically closed field. Then K is isomorphic to a finite extension of the p -adic numbers \mathbb{Q}_p . Suppose $[K : \mathbb{Q}_p] = n$ and the ramification index is e . Then there is an element $\pi \in K$ called the *generator* such that $\pi^e = p$. Let v_K be the valuation on K extending the p -adic valuation v_p on \mathbb{Q}_p such that

$$v_K(x) = \frac{1}{n} v_{\mathbb{Q}_p}(N_{K/\mathbb{Q}_p}(x)) \quad (N \text{ is the norm}).$$

Like most proofs of this kind we must treat the case when $p = 2$ separately. So first we discuss the case assuming $p > 2$.

2.1 $p > 2$

There are two cases to consider.

(1) $p \nmid n$ We show that $\mathcal{O}_K = \{x \in K : \exists y(y^{2n} = px^{2n} + 1)\}$.

Let $\alpha \in \mathcal{O}_K$. Consider the polynomial $f(Y) = Y^{2n} - (p\alpha^{2n} + 1)$. Since $f(Y) \equiv Y^{2n} - 1 \pmod{\pi}$, $f(1) \equiv 0 \pmod{\pi}$. Note that $f'(Y) \equiv 2nY^{2n-1} \pmod{\pi}$. It follows that $f'(1) \not\equiv 0 \pmod{\pi}$. Hence by Hensel's lemma there is an element y such that $y^{2n} = p\alpha^{2n} + 1$.

Now let x be an element of K such that there is y with $y^{2n} = px^{2n} + 1$. Then $v_K(y^{2n}) = 2nv_K(y)$. Suppose $x \notin \mathcal{O}_K$. Then $v_K(px^{2n} + 1) = v_K(px^{2n}) = 2nv_K(x) + 1$. Therefore, if $x \notin \mathcal{O}_K$ then $2nv_K(y)$ is even and $2nv_K(x) + 1$ odd. This is absurd. So x must be in \mathcal{O}_K .

(2) $p \mid n$ We show that $\mathcal{O}_K = \{x \in K : \exists y(y^{2n} - y = px^{2n})\}$.

Let $\alpha \in \mathcal{O}_K$. Consider the polynomial $f(Y) = Y^{2n} - Y - p\alpha^{2n}$. Since $f(Y) \equiv Y^{2n} - Y \pmod{\pi}$, we have $f(1) \equiv 0 \pmod{\pi}$. Now $f'(Y) \equiv 2nY^{2n-1} - 1 \equiv -1 \pmod{\pi}$ since p divides n . Hence $f'(1) \not\equiv 0 \pmod{\pi}$. By Hensel's lemma, there is an element y such that $y^{2n} - y = p\alpha^{2n}$.

Now suppose $y^{2n} - y = px^{2n}$ for some $x, y \in K$. We show that $x \in \mathcal{O}_K$. Note first that $v_K(px^{2n})$ is an odd integer. It is easy to see that $v_K(y^{2n} - y) = \min\{v_K(y^{2n}), v_K(y)\}$.

(i) Suppose $v_K(y^{2n}) = v_K(y)$. Then $2nv_K(y) = v_K(y)$. Hence $v_K(y) = 0$. Thus y is a unit. Then $y^{2n} - y \in \mathcal{O}_K$. Therefore $px^{2n} \in \mathcal{O}_K$ as well. It follows that $v_K(px^{2n}) = 1 + 2nv_K(x) \geq 0$. This gives us the inequation $0 > v_K(x) \geq \frac{-1}{2n}$, if $x \notin \mathcal{O}_K$. But this

contradicts the fact that $v_K(x) \in \frac{1}{n}\mathbb{Z}$.

(ii) Suppose $v_K(y) < v_K(y^{2n})$. Then $v_K(y) < 2nv_K(y)$. Hence $v_K(y) > 0$. Then as in the case (i) above, we have $px^{2n} \in \mathcal{O}_K$. Consequently this yields a contradiction as before.

(iii) Suppose $v_K(y^{2n}) < v_K(y)$. In this case, since $v_K(y^{2n} - y) = v_K(y^{2n})$ we get a contradiction immediately by checking the parity of $v_K(y^{2n})$ and $v_K(px^{2n})$.

2.2 $p = 2$

In this case, regardless whether n is either even or odd we have that $\mathcal{O}_K = \{x \in K : \exists y(y^{2n} - y = px^{2n})\}$. The same argument above works for $p = 2$.

References

- [1] A. Prestel, P. Roquette, Formally p -adic Fields, LNM 1050, Springer, 1984